SECUREDATA, Inc.
SecureUSB BT

FIPS 140-2 Non-Proprietary Security Policy
Version 1.0

Table of Contents

List of Tables

List of Figures

1 Cryptographic Module Specification

1.1 Overview

The SECUREDATA, Inc. SecureUSB BT is a multi-chip, stand-alone, cryptographic module that provides hardware-encrypted storage of user data with a USB 3.0 interface. Access to encrypted data is authenticated via the Bluetooth interface. User data is protected by 256-bit XTS-AES encryption that secures sensitive information from unauthorized disclosure in the event that the module is lost or stolen. The custom electronics within the module are encapsulated within an opaque, production grade epoxy. The module's enclosure defines the cryptographic boundary[1].

The data encryption key (DEK) and other critical security parameters (CSPs) are generated by a NIST approved DRBG[2] within the module when it is first used. The seed for the DRBG is also produced within the module from a hardware-based, entropy generator.

The user interface for the module is three (3) status-indicators LEDs. The LEDs are each a different color, red, green, and blue.

1 Excluded components within the cryptographic boundary include passive electronic components, LEDs, and a Bluetooth radio controller, BlueNRG-MSCSP HW V4.1 with firmware version 7.2c.

2 *SP 800-90Ar1 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. NIST. (June 2015).

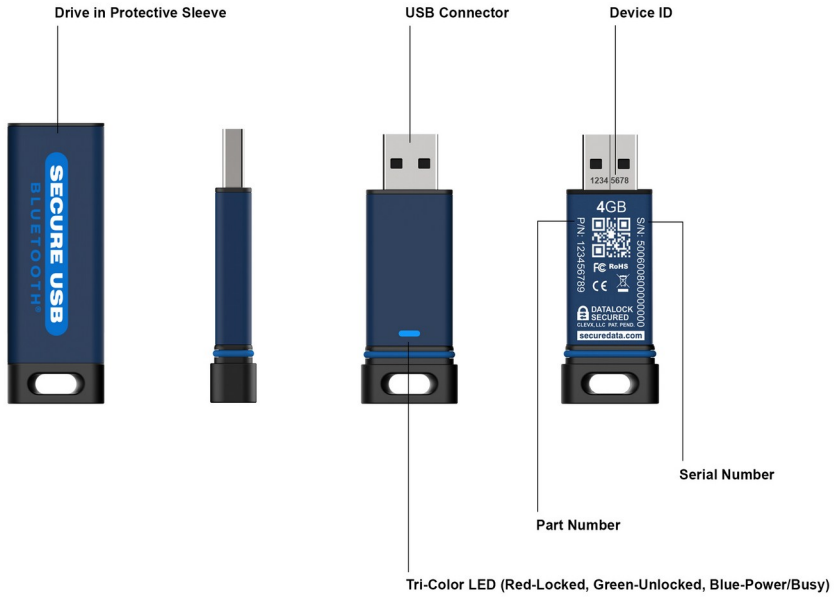

Figure 1: SecureUSB BT

Hardware Part Numbers	Firmware Versions (implemented on all hardware versions)
SU-BT-BU-4 SU-BT-BU-8 SU-BT-BU-16 SU-BT-BU-32 SU-BT-BU-64	Each module has one each of Firmware A and Firmware B. *Firmware A* V1.01.10 *Firmware B* V2.0.8 or V2.4 (no security relevant differences)

Table 1: Module Hardware and Firmware Versions

1.2 FIPS Security Level

The module meets the overall requirements for FIPS 140-2[3] Level 3.

FIPS Area	FIPS Security Requirement	Level
1	Cryptographic Module Specification	3
2	Module Ports and Interfaces	3
3	Rôles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	*n/a*
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	*n/a*

Table 2: FIPS Security Level

3 *FIPS 140-2 – Security Requirements for Cryptographic Modules*. NIST. (December 2002).

1.3 Mode of Operation

The module operates only in a FIPS approved mode. Approved mode is indicated by the three status-indicator LEDs illuminating one at a time, green, blue, and then red when the module is powered on. This indication means that firmware integrity checks and KATs have successfully passed.

To meet the requirements for FIPS 140-2 Level 3, the module enforces the following security rules:

- The cryptographic module provides two distinct operator rôles: User and Cryptographic Officer (CO).
- The cryptographic module provides identity-based authentication.
- When the module has not been placed in a valid rôle or is in an error state, the operator shall not have access to any cryptographic service.
- The operator is capable of commanding the module to perform self-tests at any time by cycling the power.
- Data output is inhibited during self-test, zeroization, key generation, and authentication.
- No CSPs are output from the module in any form.
- Each unique AES GCM/IV pair is used for one and only one secure communication session.
- Each secure communication session is established between exactly two entities.
- The module cannot establish a secure communication session with another, identical module.

2 Module Ports and Interfaces

The cryptographic module exposes the following physical ports and logical interfaces:

Physical Port	Logical Interface	Description
USB Data	Data input Data output Control input Status output	The USB Data port connects the module to the host computer. It is used to exchange decrypted user data as well as control and status information for the USB protocol. When the drive is locked the USB interface is disabled.
Bluetooth	Control input Status output Data input Data output	User and CO Password received and module status information transmitted via the Bluetooth port.
Red, green and blue LEDs	Status output	Refer to Table 4 for details.
USB Power	External power	The USB VBUS (+5VDC) powers the module and embedded storage component.

Table 3: Module Ports and Interfaces

LED Behavior[4]	Module State	Status Description
LEDs illuminate one at a time, green, blue, and then red. Red remains lit.	Connected to USB power	Module powered-on with all LEDs operational. Firmware integrity tests and KATs have passed.
LEDs illuminate continuously in circling pattern, red then green then blue.	Failed	Module in error state.
Red LED illuminated	Locked	Module locked. User data secure.
Green LED illuminated	Unlocked	Module unlocked. DEK is unobfuscated. USB interface with host has not enumerated with the host computer.
Green and blue LED illuminated	Connected	Module unlocked and connected to host computer.
Green LED illuminated. Blue LED blinking	Connected	Module unlocked and connected to host computer. There is an active data transfer with host computer.

Table 4: LED Status Indications

To verify that the module is in good working order, power it on by connecting it to a USB power source. The three status indicator LEDs will blink one at a time and once each, green, blue, and then red, indicating that firmware integrity tests and KATs have passed successfully

4 Because the module is powered from USB, the LED indicators are valid only when when the module is connected to a USB port.

3 Rôles, Services, Authentication, and Identification

3.1 Rôles and Identification

The module implements level 3, identity-based authentication with two distinct rôles, one User identity and one Crypto-Officer identity.

Identity	Identification	Authentication Data	Description
User[5]	User chooses ASCII value '1' for User identification.	7-15 character Password	User has full access to all User services.
CO	CO chooses ASCII value '0' for CO identification.	7-15 character Password	CO has full access to all CO services.

Table 5: Module Rôles

3.2 Module Initialization

A new module comes from the factory initialized with a default User Password of '11223344'. This factory default password must be changed before storing confidential data on the module[6]. No CO Password is defined for a factory initialized module. In the factory initialized configuration, the module is ready for operation in a FIPS approved mode.

If the module is zeroized, there will be neither a User Password nor a CO Password defined and there will be no DEK. The module must be initialized before it will operate in an approved mode. From this state, either a User or a CO Password may be defined first.

5 In the case where the User password is defined but no CO password is defined, the User identity behaves as a combined User/CO identity.

6 Per FIPS 140-2 §4.3.3, the default password does not meet the strength of the authentication requirement because it may be guessed in one attempt.

3.3 Services

Identity	Service	CSP Access
CO	Set CO Password	Read, Execute, and Write Change CO Password, CO salt, and CO KEK. Create DEK using CTR-DRBG state (seed, V, key) if one is not defined.
	Set User Password	Read, Execute, and Write Change User Password, User salt, and User KEK.
	Zeroize User Password	Zeroize Zeroize User salt and User KEK.
	Erase private partition data	Read, Execute, and Write Change CO salt and CO KEK. Create DEK using CTR-DRBG state (seed, V, key). Zeroize Zeroize User salt and KEK.
	Open private partition for read/write access to user data	Read and Execute Read CO salt and CO KEK. Unobfuscate DEK.
	Lock private partition to prevent read/write access to user data	Zeroize Zeroize DEK in RAM.
	Read or write private partition with user data	Read Use DEK to encrypt and decrypt user data.
	Configure idle timeout lock	None
	Configure Remote Management	None
	Change nickname	None
	Configure Step-Away lock	None
User	Set CO Password when none exists	Read, Execute, and Write Change CO Password, CO salt, and CO KEK.
	Set User Password	Read, Use, and Write Change User Password, User salt, and User KEK. Create DEK using CTR-DRBG state (seed, V, key) if one is not defined.
	Open private partition for read/write access to user data	Read and Execute Read CO salt and CO KEK. Unobfuscate DEK.
	Lock private partition to prevent read/write access to user data	Zeroize Zeroize DEK in RAM.
	Read or write private partition with user data	Read and Execute Use DEK to encrypt and decrypt user data.
	Configure idle timeout lock	None
	Change nickname	None
	Configure Step-Away lock	None

Identity	Service	CSP Access
Unauthenticated	Show locked/unlocked status	None
	Show whether or not drive is initialized	Read and Execute Verify validity of either User salt or CO salt.
	Show whether or not User Password is defined	Read and Execute Verify validity of User salt.
	Show whether or not CO Password is defined	Read and Execute Verify validity of CO salt.
	Run self-tests	None
	Factory reset (zeroize) module and erase private partition data	Zeroize Zeroize all CSPs.
	Query firmware version	None
	Authentication	Read, Execute, and Write Create and read ECC-CDH Private Key, Session Master Secret, AES-GCM Key/IV

Table 6: Services Available in FIPS Approved Mode

3.4 Authentication

The Crypto Officer and User rôles authenticate via the Bluetooth interface. The module does not output CO or User authentication data outside of the cryptographic boundary. Communication via the Bluetooth interface is protected by encryption. Messages are encrypted and authenticated with AES-GCM (Cert. #5397). Cryptographic keys are established per SP 800-56Ar2 scheme C(0s, 2e, ECC CDH), with the primitive tested by CVL (Cert. #1857) and the single step KDF per SP 800-56Ar2 Section 5.8.1. These keys are used for key derivation using KBKDF (Cert. #201) in Counter Mode, which relies on AES-CMAC (Cert. #5366) and HMAC-SHA-1 (Cert. #3554) per SP 800-108, to create the AES-GCM keys.

The Password, from either the User or the CO, is an input to PBKDFv2 that produces the Key Encryption Key (KEK) for that rôle. The KEK is used by the non-approved cryptographic Synthetic Initialization Vector[7] (SIV) algorithm to obfuscate the DEK. SIV is constructed using AES CTR (Cert. #5366) and AES CMAC (Cert. #5366). Unobfuscating the DEK requires the same Password that was given to PBKDFv2 when the DEK was obfuscated.

The authentication strength for the module is determined by the Password. There are more than 10 million (10^7) Password combinations with a minimum length of seven (7) bytes. This lower bound is derived by using only the ASCII decimal digits `'0'-'9'` in the Password, seven bytes and ten choices per byte. Because the Password may be composed of UTF-8 characters, the length in characters may be fewer than seven. The module enforces the minimum Password length in bytes.

UTF-8[8] character encodings may span from one to four bytes. For UTF-8 characters to supply more combinations of Passwords than the ASCII decimal digits, there must be at least 3.4 variable bits in each encoded byte[9]. In a single byte UTF-8 character, there are seven (7) variable bits where we require at least 3.4 to meet the lower bound. In two byte characters, there are eleven (11) variable bits where we require at least 6.8. In three byte characters, there are 16 variable bits where we require at least 10.2. In four byte characters, there are 21 variable bits where we require at least 13.6. Or, to put it a different way, every byte in a UTF-8 character has at least 5 variable bits which is more than the minimum of 3.4 bits necessary to meet the lower bound. Therefore, passwords encoded in seven bytes of UTF-8 characters will

7 Harkins, D. *Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)*. IETF. (October 2008)

8 https://www.unicode.org/versions/Unicode11.0.0

9 At least 3.32 binary bits are needed to uniquely represent ten distinct values; $2^{3.32} \cong 10$

have at least 10^7 different combinations and the chances of a successful random guess is less than one in 10,000,000 (10^{-7}).

The module protects against brute-force attempts to guess a rôle's PIN/Password by permitting no more than ten (10) consecutive incorrect guesses before locking out that rôle. Incorrect PIN/Password attempts are counted independently for each rôle. The probability of an attacker correctly guessing a PIN/Password in any time period[10], such as a one-minute interval, is 10^{-6} or 1 chance in 1,000,000.

10 The FIPS 140-2 standard stipulates that "*For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 (10^{-5}) that a random attempt will succeed or a false acceptance will occur.* " In this product, a single successful attempt to guess a PIN/Password has a probability less than one in 10,000,000 (10^{-7}). Ten guesses has a probability of one in 1,000,000 ($10*10^{-7}$ or 10^{-6}) of success. The standard requires that the probability of a successful guess be less than one in 100,000 (10^{-5}) in a one-minute period. The authentication mechanism of this module is better than the standard requires, over any time interval—including a one-minute period. A probability of one in 1,000,000 (10^{-6}) is less likely than one in 100,000 (10^{-5}).

4 Physical Security

The multi-chip standalone cryptographic module includes the following physical security mechanisms, conforming to FIPS 140-2 Level 3 requirements:

1. Production grade components
2. Hard, opaque, tamper-evident enclosure with embedded, hard epoxy covering all security relevant components. Epoxy hardness was tested at ambient temperature meaning that no assurance is provided for Level 3 hardness conformance at any other temperature.
3. Memory protection enabled to prevent read-out of firmware, RAM, or NVRAM

The operator is responsible for inspecting the module on each use for evidence of tampering. If the module is physically compromised it is no longer guaranteed to provide FIPS protections and should be replaced.

5 Operational Environment

The FIPS 140-2 Operational Environment (Area 6) requirements for the module are not applicable because the device does not contain a modifiable operational environment.

6 Cryptographic Key Management

6.1 Cryptographic Algorithms

Algorithm	Modes	Key Sizes	Reference	CAVP Cert.	Use
AES	XTS[12]	256	NIST SP 800-38E[13]	AES 5942	Encryption of user data within storage application only
AES	ECB CMAC CTR	128 256 (ECB only)	FIPS 197[14] NIST SP 800-38A[15]	5366	Block cipher basis of CTR-DRBG. Algorithmic basis of SIV.
AES	ECB GCM	128	FIPS 197 NIST SP 800-38A NIST SP 800-38D[16]	5397	AES-ECB is the block cipher basis for AES-GCM which is used to encrypt Bluetooth messages
CKG	-	256	NIST SP-800-133[17]	Vendor Affirmed	The unmodified output of the DRBG is used for generating symmetric and asymmetric keys.
DRBG	AES-CTR	256	NIST SP 800-90A[18]	2077	Random number generator for encryption keys and salts
ECDSA	-	P-256	FIPS 186-4[19]	1428[20]	ECC key generation for SP 800-56Ar2 key agreement
HMAC	HMAC-SHA-1	160	FIPS 198-1[21]	3554	Algorithmic basis of PBKDFv2
KAS	ECC CDH	P-256	NIST SP 800-56Ar2[22]	Vendor Affirmed (CVL 1857)	Key agreement for securing Bluetooth messages using ECC CDH Primitive (CVL Cert #1857) for sharing secret computation with ECDSA (Cert #1428) as a prerequisite for ECC key pair generation, and SHS (SHS Cert #4308) as a prerequisite for single-step key generation.
KBKDF	AES-CMAC	128	NIST SP 800-108[23]	201	Derivation of keys for Bluetooth message encryption
PBKDFv2	HMAC-SHA-1	-	NIST SP 800-132[24]	Vendor Affirmed	KEK generation. Password is the same as the User/CO Password with a minimum length of 7 characters. Algorithm conforms to FIPS 140-2 Implementation Guidance (IG) D.6: the module supports option 2a as documented in SP 800-132 § 5.4.
SHS	SHA-1	-	FIPS 180-4[25]	4308	Algorithmic basis of HMAC-SHA1

Table 7: FIPS Approved Algorithms

12 ECB mode is included in the CAVS certificate, but is used by no services in the module.
13 *SP 800-38E – Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*. NIST. (January 2010).
14 *FIPS 197 – Advanced Encryption Standard (AES)*. NIST. (November 2001).
15 *SP 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. NIST. (December 2001).
16 *SP 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. NIST. (November 2007).
17 *SP 800-133 – Recommendation for Cryptographic Key Generation*. NIST. (December 2012).
18 *SP 800-90Ar1 – Recommendation for Random Number Generation Using Determinstic Random Bit Generators*. NIST. (June 2015).
19 *FIPS 186-4 – Digital Signature Standard (DSS).* NIST. (July 2013).
20 Certificate #1428 covers only key pair generation. Signature and verification functions are not used.
21 *FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC)*. NIST. (July 2008).
22 *SP 800-56Ar2 – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*. NIST. (May 2013).
23 *SP 800-108 – Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*. NIST. (October 2009).
24 *SP 800-132 – Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*. NIST. (December 2010).
25 *FIPS 180-4 – Secure Hash Standard (SHS)*. NIST. (August 2015).

Algorithm	Strength	Use
NDRNG	Module generates cryptographic keys with a minimum security strength of 256 bits.	Entropy source for seed to CTR-DRBG

Table 8: FIPS Allowed Algorithms

Algorithm	Use
SIV[26] (no security claimed)	Per FIPS 140-2 IG §1.23, SIV is a non-approved cryptographic algorithm. It is allowed in FIPS approved mode. It is not a security function. *"Cryptographic keys and CSPs encrypted using a non-approved algorithm or proprietary algorithm or method are considered in plaintext form, within the scope of this standard [FIPS 140-2]."* SIV is used during authentication and meets all authentication strength requirements. SIV uses the CO KEK and User KEK, derived from the CO or User PIN/Password via KBKDFv2, to obfuscate and unobfuscate the DEK.

Table 9: FIPS Non-approved Algorithms

6.2 Critical Security Parameters

The module does not input or output private or secret cryptographic keys. Cryptographic keys are established per SP 800-56Ar2 scheme C(0s,2e,ECC_CDH) and conforming to SP 800-133. KEKs are derived using PBKDFv2[27] and are only used as part of the module's data storage application. Public/private key pairs are ephemeral, used for one and only one key agreement, and destroyed immediately after use.

26 Harkins, D. Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES). IETF. (October 2008). SIV is a Authenticated Encryption algorithm codified by the IETF in RFC-5297. NIST has not analyzed this algorithm, so it is specified here as non-approved for the purposes of FIPS 140-2. Obfuscation of the DEK depends on the user's PIN/Password and SIV to prevent the plaintext DEK from being stored in NVRAM. NIST characterizes the storage of the DEK as plaintext explicitly because SIV is non-approved.

27 Per FIPS SP800-132 and FIPS140IG § D.6, the materials derived from PBKDFv2 are used only for "protection of electronically-stored data or for the protection of data protection keys."

Parameter	Description	Source	Storage	Creation / Destruction
CTR-DRBG state (seed, V, key)	Generating random values for CSPs 256 bit output (full entropy)	NDRNG and CTR-DRBG	RAM	Created when DRBG is seeded which is every time the module initializes
				Destroyed on lock, connect, successful generation of CSPs, power-off, and zeroization
User Password	Input to PBKDFv2 to allow generation of the User KEK Strength of 7-15 bytes	Keypad entry	RAM	Created by User
				Destroyed on lock, unlock, timeout, and power-off
CO Password	Input to PBKDFv2 to allow generation of the CO KEK Strength of 7-15 bytes	Keypad Entry	RAM	Created by CO
				Destroyed on lock, unlock, timeout, and power-off
User Salt	Input to PBKDFv2 to generate key to obfuscate DEK 128 bit value	CTR-DRBG	NVRAM	Created when User changes Password
				Destroyed on Password change, zeroization
CO Salt	Input to PBKDFv2 to generate key to obfuscate DEK 128 bit value	CTR-DRBG	NVRAM	Created when CO changes Password
				Destroyed on Password change, zeroization
XTS-AES DEK	Encryption and decryption of user data XTS-AES 256 bit key	CTR-DRBG	RAM	Created when first password, either User or CO, is set
				Destroyed on lock, timeout, entering low-power mode, power-off, and zeroization
User KEK	Obfuscation and unobfuscation of DEK SIV AES 128 bit key	User Password, User Salt, and PBKDFv2	RAM	Created before obfuscation or unobfuscation of the DEK.
				Destroyed immediately after use.
CO KEK	Obfuscation and unobfuscation of DEK SIV AES 128 bit key	CO Password, CO Salt, and PBKDFv2	RAM	Created before obfuscation or unobfuscation of the DEK.
				Destroyed immediately after use.
ECC-CDH Private Key	Bluetooth Message Encryption ECC P-256 256 bit key	CTR-DRBG	RAM	Generated when Bluetooth client requests secure channel
				Destroyed when secure channel established
Session Master Secret	Bluetooth Message Encryption 256 bit secret	ECC-CDH Key Agreement	RAM	Created when secure channel established
				Destroyed when secure channel session ends

AES-GCM Key / IV	Bluetooth Message Encryption AES key 128 bits IV 96 bits	Session Master Secret and KDF-AES-CMAC	RAM	Created when secure channel established or when secure channel is rekeyed
				Destroyed when secure channel session ends

Table 10: Critical Security Parameters

Parameter	Use	Source	Storage	Creation / Destruction
ECC-CDH Public Key	Bluetooth Message Encryption ECC P-256 256 bit key	ECC Primitive	RAM	Generated when Bluetooth client requests secure channel
				Destroyed when secure channel established
ECC-CDH Peer Public Key	Bluetooth Message Encryption ECC P-256 256 bit key	Remote Bluetooth Client	RAM	Generated when Bluetooth client requests secure channel
				Destroyed when secure channel established

Table 11: Public Security Parameters

6.3 Zeroization of Critical Security Parameters

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The module initiates an erase cycle to zeroize CSPs stored in NVRAM. Copies of CSPs in RAM are erased by setting the memory to zeros. This process occurs when the module is factory reset or when the module detects a brute-force attack.

There are two kinds of brute-force attacks. Ten consecutive failed attempts to unlock the module as the User is the first type of brute-force attack and will zeroize the User CSPs. After this type of attack, the CO will be able to unlock the module, recover user data, and permit the setup of a new User Password. However, if there is no CO Password, the user data partition will be erased leaving the module in the factory reset state with an erased use data partition.

The second kind of brute-force attack is against the CO Password. Ten consecutive failed attempts to unlock the module as CO will zeroize all CSPs for both the CO and User rôles,

including the DEK. The module will be left in the factory reset state with an erased user data partition.

6.3.1 Zeroization via Factory Reset

A Factory Reset will erase all CSPs, settings, and user data from the module. After this operation, the operator must initialize the module per section 3.2 to return it to a FIPS approved mode.

Starting with the module connected to USB power:

1. Invoke the **FactoryReset** service.
2. Query **Status** until operation is complete.
3. Initialize module by creating a new PIN/Password and reformatting the drive.

7 EMI/EMC Regulatory Compliance

This module conforms to the EMI/EMC requirements specified by Title 47 of the Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use). The module incorporates a Bluetooth radio with FCC ID 2AOXICAUSB which is excluded from the EMI/EMC requirements for FIPS.

8 Self-Tests

When the module powers on, it performs a sequence of self-tests. If any of these tests fails, the drive will enter an error state. The module cannot perform any cryptographic services and is not usable in this state. The module also performs conditional self-tests. The only way to clear a module error state is to cycle the power. Self-tests are summarized in Table 12.

Test Category	Test Name	When Executed	Failure Indications
Firmware Integrity	Firmware CRC-32	Module power-on	Module illuminates no LEDs.
	Firmware CRC-16	Module power-on	Module fails to mount to host PC after successful unlock and returns to locked state.
Known Answer	DRBG Cert. #2077 KAT[28]s CTR-DRBG Instantiate CTR-DRBG Generate	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	PBKDFv2 combined KAT[29] HMAC SHA-1 Cert. #3554 SHA-1 Cert. #4308	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	AES #5366 KATs AES ECB encrypt Cert. #5366 AES ECB decrypt Cert. #5366 AES CMAC Cert. #5366	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	XTS-AES Cert. #AES 5942 KATs AES-XTS encrypt AES-XTS decrypt	Module power-on	Module fails to mount to host PC after successful unlock. Module automatically locks and illuminates red LED.
	AES-GCM Cert. #5397 KATs AES-GCM authenticated encrypt AES-GCM authenticated decrypt	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
	SP 800-56Ar2 KAS KATs per IG 9.6 Primitive 'Z' Computation KAT CVL Cert. #1857 SHA-1 KDF KAT Cert. #4308 AES CMAC (KDF Prerequisite) KAT Cert. #5366	Module power-on	LEDs illuminate in continuously circling pattern, red then green then blue.
Conditional	ECC Partial Public-Key Validation; Assurance per SP 800-56Ar2 §5.6.2.2.2	Use of SP 800-56Ar2 Key Agreement	LEDs illuminate in continuously circling pattern, red then green then blue.
	NDRNG Conditional Test	Use of NDRNG	LEDs illuminate in continuously circling pattern, red then green then blue.
	XTS-AES; Key validity per IG A.9 CAVP #AES 5942	Creation of DEK	Module fails to mount to host PC after successful unlock. Module automatically locks and illuminates red LED.

Table 12: Module Self-Tests

28 KATs are Health tests per section 11.3 of SP800-90A. The CRNGT per section 4.9.2 of FIPS 140-2 is not necessary per IG 9.8.

29 A single KAT for HMAC incorporates the SHA test.

9 Mitigation of Other Attacks

The module has not been designed to mitigate attacks not addressed by the security requirements of FIPS 140-2.

10 Glossary of Terms and Acronyms

Term	Definition
AES	Advanced Encryption Standard
AES-GCM	AES Galois Counter Mode cipher used to encrypt Bluetooth messages
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CTR-DRBG	Counter-Mode Deterministic Random Byte Generator
DEK	Data Encryption Key
DRBG	Deterministic Random Byte Generator
ECB	Electronic Code Book
ECC	Elliptical Curve Cryptography
ECC-CDH	ECC Cofactor Diffie Hellman
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Protocol
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
KDF	Key Derivation Function
KEK	Key Encryption Key
LED	Light Emitting Diode
NDRNG	Non-deterministic Random Number Generator; module entropy source
NIST	National Institute of Standards and Technology

NVRAM	Non-volatile Random Access Memory
PBKDFv2	Password Based Key Derivation Algorithm Version 2
Password	User's secret authentication character sequence
RAM	Random Access Memory
Salt	Random value used to improve security of cryptographic algorithms
SATA	Serial AT Attachment
SHA-1	Secure Hash Algorithm 1
SHS	Secure Hash Standard
SIV	Synthetic Initialization Vector
USB	Universal Serial Bus
XTS-AES	AES cipher mode used to encrypt user data in mass storage
Zeroization	The process of erasing cryptographic security keys and parameters